Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Relocation Application

U.S. Department of Commerce Privacy Threshold Analysis

Office of the Secretary/Relocation Application

Unique Project Identifier: An EAS OS-059 Application

Introduction: The moveLINQ software is a commercial-off-the-shelf (COTS) web based application designed to manage the federal government travel relocation process. To improve and automate the relocation process Department-wide, DoC recently acquired the moveLINQ application developed by moveLINQ, LLC. This software was previously maintained by the National Institute of Standards & Technology (NIST). As a part of a phased-in approach to using the application department-wide, the system will now be maintained by the CBS Solutions Center in Gaithersburg, MD and housed at the DoT/FAA/ESC datacenter in Oklahoma City, OK. Personnel at DoT/FAA/ESC datacenter will not have access to the application's data. There will be no business process or system changes, only the location of the application is changing. This move will precede the possible inclusion of other bureaus on the moveLINQ application but this PIA only includes NIST's use of the moveLINQ application.

The moveLINQ application is an application within the EAS (OS-059) boundary. This PIA only addresses the moveLINQ application. The moveLINQ application tracks all individual relocation expenses associated with moving an employee and their family members. It fully automates the requirements of the Federal Travel Regulations - chapter 302, the Department of State Standardized Regulations, and IRS Publications related to relocation payments. The application manages and tracks all aspects of government change of station and taxable Temporary Duty (TDY) travel allowances. Users from the NIST Travel Group will manually enter information regarding relocation activities of employees and the system will calculate the appropriate per-diem rates as well as tax information related to the move. This information stored is tied to a unique identification number (system generated) for each relocation. The application will communicate with the Commerce Business Systems (CBS) using standard interface connection mechanisms. The moveLINQ application will be used to record and process relocation actions for bureau employees within the DoC.

The moveLINQ application has the functionality to create file exports to create required tax forms to provide to the IRS and employees for annual tax filing. This functionality is currently not used and it requires purchasing additional software. This PIA will updated to reflect this process if the functionality is used in the future.

The moveLINQ application will potentially hold name, home address (current and future relocation address); federal and state taxes paid in the name of employee being located, names of the employee's children and their DOB(s), spouses\partners name, supporting documentation

that may have last four digits of personal credit card numbers, driver's license numbers, and, vehicle identifier. The overall FIPS-199 impact level for this application is Moderate.

Legal authority\regulations that applies to the collection of this data are (but not limited to);

- Department of Commerce Privacy Act Systems of Records, Dept-9 Travel Records (Domestic and Foreign) of Employees and Certain other Persons. (http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-9.html)
    - Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966
- Department of Commerce Privacy Act Systems of Records, DEPT-18 Employees Personnel Files Not Covered By Notices of Other Agencies (http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html)
    - Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

_X_ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes	X	f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ATO is current and was granted when application was hosted at NIST. Managed now by CSC and will be hosted at ESC/FAA datacenter in Oklahoma City, OK. It will be an application within EAS OS-059 which last received an ATO on 8/11/16					

_ This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
____ Contractors working on behalf of DOC
_X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to ~~C. Suite~~ Relocation application for and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of System Owner (SO): Gay Shrum

Signature of SO: Gay Shrum Date: 3/9/2017

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: JUN KIM Digitally signed by JUN KIM DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988 Date: 2017.04.14 12:20:45 -04'00' Date: 4/14/2017

Name of Authorizing Official (AO): Lisa Casias

Signature of AO: Lisa Casias Date: 5/4/17

Name of Bureau Chief Privacy Officer (BCPO): Kathleen Gioffre, OS Privacy Officer

Signature of BCPO: KATHLEEN GIOFFRE Digitally signed by KATHLEEN GIOFFRE DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=KATHLEEN GIOFFRE, 0.9.2342.19200300.100.1.1=13001000075444 Date: 2017.06.19 10:41:25 -04'00' Date: _____